MultiVoice packet processing

MultiVoice voice and data are processed using User Datagram Protocol (UDP) packets. UDP is a protocol within the TCP/IP protocol suite that is used in place of TCP for processing real-time audio and video traffic. UDP is used with Real-time Transport Protocol (RTP) to provide delivery, packet sequence checking, and error notification for MultiVoice call processing.

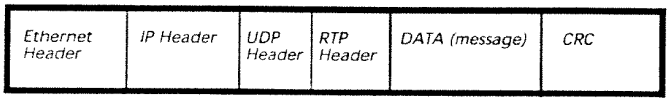
Voice over IP (VoIP) call data is compressed into frames assembled inside RTP packets. Each RTP packet is wrapped within a UDP packet and includes timestamping and synchronization information in its header for proper reassembly of the voice frames at the receiving end.

In a UDP/IP stack, the RTP header is created first and then the packet is moved down the stack to UDP and IP. UDP hands over these packets to the IP protocol layer along with the IP address of the destination node.

At the IP layer, the target address information for the destination gateway is processed, then passed to the Ethernet layer which establishes the data link between the two MultiVoice Gateways; completing the connection between the packet network and the PSTN.

Figure 1-2 illustrates how each MultiVoice packet is formatted for transmission across the packet network.

Figure 1-2. MultiVoice packet format



For more details on MultiVoice packet processing see Appendix A, "MultiVoice Packet Processing."

Supported audio codecs

MultiVoice provides support for the following audio compression/decompression algorithms (codecs) as defined by the International Telecommunications Union Telecommunications sector standards (Series G) for telephonic audio transmission:

Audio codec	Description
G.711	This algorithm transmits and receives a-law and μ–law pulse code modulation (PCM) voice signals at digital bit-rates of 48Kbps, 56Kbps, and 64Kbps. Digital telephone sets on digital PBXs and ISDN channels use this algorithm. Support is required by the H.323 standard. MultiVoice supports both G.711 A-law and G.711 μ–law.
G.723.1	This algorithm performs speech compression/decompression using a low bit rate—5.3Kbps or 6.3Kbps—output quality. This codec is designed specifically for voice transmission over low bit-rate links (greater than 56Kbps). MultiVoice supports this codec at both bit-rates.

Audio codec	Description
G.728	This algorithm performs speech compression/decompression at 16Kbps using low-delay code excited linear predictive methods, with a frame size of 2.5 milliseconds. MultiVoice implements this codec using a frame size of 5 milliseconds. It uses the same bitstream as the ITU-T standard and allows speech processed by a MultiVoice Gateway to be processed by any other gateway that supports the G.728 standard.
G.729(A)	This Conjugate Structure, Algebraic Code Excited Linear Predictive (CS-ACELP) algorithm is used for compression/decompression of speech at 8Kbps, as defined by the ITU-T Standard G.729, with Annex A.
Full-rate GSM	This algorithm is a voice encoder/decoder standard for cellular communications. It compresses the speech samples from 64Kbps PCM to 13.2Kbps, requiring less network than G.711 a-law/μ–law. European, Japanese and Australian cellular communications systems follow this standard, and certain Web phone applications support it. Full-rate GSM uses a speech frame size of 160 samples (20 msec) and the encoder produces 33 bytes per frame. The decoder produces 160 samples (20msec) of speech from the 33-byte encoder output. This algorithm also supports silence detection and comfort noise generation for Full-rate GSM.

H.323 implementation

MultiVoice implements the H.323 standards defined for both gateways and gatekeepers. Gateways connect the PSTN to the IP-based network. Calls originate at a MultiVoice Gateway and travel across the IP network, which are then routed to a second MultiVoice Gateway that is connected to the PSTN and, then ultimately, to the destination phone. The gatekeeper manages the network, supporting all gateways, user profiles, and authentication. The MultiVoice Access Manager (MVAM) performs the gatekeeper functions for a MultiVoice network.

Supporting the H.323 direct-call model for Voice over IP networks, MultiVoice implementation includes

- Integrating PSTN and packet networks to complete calls
- Using primary and secondary gatekeepers
- Using overlapping gateway coverage areas

Integrating PSTN and packet networks

A MultiVoice network integrates both the PSTN and packet networks. Two gateways connect Caller A to Caller B. An NT or Solaris-based server running MVAM is the gatekeeper.

In Figure 1-3, when Caller A dials Caller B, the following high-level events occur:

1 Caller A dials Gateway 1 and enters the PIN authentication (if required) and Caller B's phone number.

2 Gateway 1 establishes a session with the gatekeeper.

3 Gateway 1 forwards the phone number and PIN authentication to the gatekeeper.

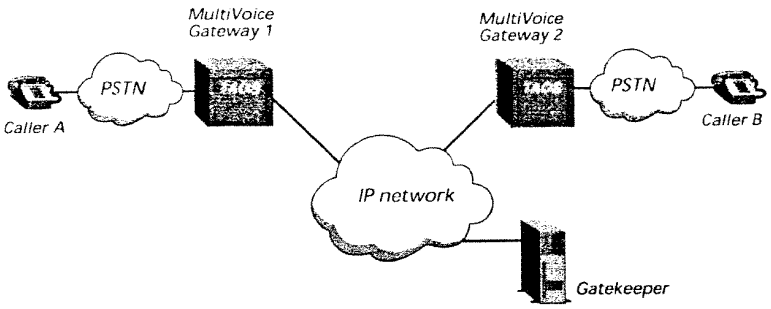
4 The gatekeeper authenticates Caller A and, if authentication is successful, forwards the IP address of Gateway 2 to Gateway 1.

5 Gateway 1 establishes a session with Gateway 2.

6 Gateway 2 forwards the call request to Caller B.

When Caller B answers the phone (goes off-hook), voice traffic is transmitted in IP packets between Gateway 1 and Gateway 2 using RTP protocol.

Figure 1-3. Example of a MultiVoice network



If the callers in Figure 1-3 used a traditional voice communications network, Caller A would require a long-distance carrier's services to reach Caller B. But, Caller A is in Gateway 1's coverage area, and can reach the gateway with a local call. The IP-routed network performs the same function as a long-distance carrier's circuit-switched network.

Coverage areas

Each MultiVoice Gateway services a *coverage area*. The coverage area consists of a group of telephone numbers that may dial and receive calls through a particular gateway. Coverage areas for each gateway are defined by assigning dial strings, such as country codes, area codes, country code/area code combinations, area code/exchange combinations, or complete telephone numbers, to a database on the gatekeeper.

Inclusion areas

Individually, each of the telephone numbers and dial strings assigned to a coverage area represents an individual *inclusion area*. Together, these inclusion areas represent the coverage area for a MultiVoice Gateway. For example, an inclusion area could be specified by the partial telephone number *1732*. This number is composed of a country code of *1* and area code of *732*. A gateway with this inclusion area would cover all telephone numbers within the 732 area code.

Overlapping gateway coverage areas

In a MultiVoice network with overlapping gateway coverage areas, two or more gateways can process incoming calls to telephone numbers in the same coverage area. The MVAM allows you to assign the same inclusion areas, defined by country codes, area codes, country code/area code combinations, area code/exchange combinations, or complete telephone numbers, to two or more gateways, creating overlapping coverage areas.

Identical coverage areas may be configured on the gatekeeper for each MultiVoice Gateway in the group. This type of network configuration provides for dynamic call management and allow the gatekeeper to perform call load-leveling across a group of gateways.

Figure 1-4 illustrates a MultiVoice network with overlapping coverage areas. Two gateways provide coverage to area code 516. An NT or Solaris-based server running MVAM is the gatekeeper. When Caller A dials Caller D, Caller C dials Caller B, and both dialed phone numbers are part of the same coverage area, the following high-level events occur:

1 Caller A dials Gateway 1, and enters the PIN authentication (if required) and Caller D's phone number.

2 Gateway 1 establishes a session with the gatekeeper.

3 Gateway 1 forwards the phone number and PIN authentication to the gatekeeper.

4 The gatekeeper attempts to authenticate Caller A and, if successful, identifies all the MultiVoice Gateways that support the coverage area for Caller D's phone number.

5 The gatekeeper forwards the IP address of Gateway 2 to Gateway 1.

6 Gateway 1 establishes a session with Gateway 2.

7 Gateway 2 forwards the call request to Caller D.

8 Now, Caller C dials Gateway 1, and enters his or her PIN authentication (if required) and Caller B's phone number.

9 Gateway 1 establishes a session with the gatekeeper.

10 Gateway 1 forwards the phone number and PIN authentication to the gatekeeper.

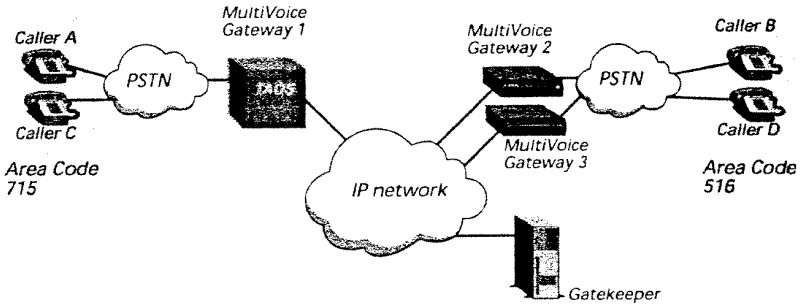
11 The gatekeeper attempts to authenticate Caller C and, if successful, identifies the MultiVoice Gateways that support the coverage area for Caller B's phone number.

12 This time the gatekeeper forwards the IP address of Gateway 3 to Gateway 1.

13 Gateway 1 establishes a session with Gateway 3.

14 Gateway 3 forwards the call request to Caller B.

Figure 1-4. Example of a MultiVoice network with overlapping coverage areas



In Figure 1-4, the gatekeeper, having already routed a call from Caller A to Caller D through Gateway 2, determines that the call from Caller C to Caller B should be routed through Gateway 3 instead of Gateway 2 to keep the call volume balanced.

Since MultiVoice uses one port per call, the gatekeeper attempts to assign calls to each gateway based upon port availability, alternating call assignments between covering gateways.

Using primary and secondary gatekeepers

Figure 1-5 shows an example of a MultiVoice network that uses primary and secondary gatekeepers to manage VoIP network operations. The VoIP network configuration in Figure 1-5 provides the MultiVoice network with redundant call-management capability.

Each MultiVoice Gateway may be configured to register with a secondary gatekeeper when it cannot register with the primary gatekeeper. This enables call processing to continue in the event that the primary gatekeeper cannot be reached by a gateway (redundancy).

As illustrated in Figure 1-5, two MultiVoice gateways can connect Caller A to Caller B. Either of the NT or Solaris-based servers running MVAM can be the gatekeeper.

When Caller A dials Caller B, the following high-level events occur:

1 Caller A dials Gateway 1 and enters the PIN authentication (if required) and Caller B's phone number.

2 Gateway 1 attempts to register with it's primary gatekeeper.

If the registration fails, Gateway 1 attempts to register with its secondary gatekeeper.

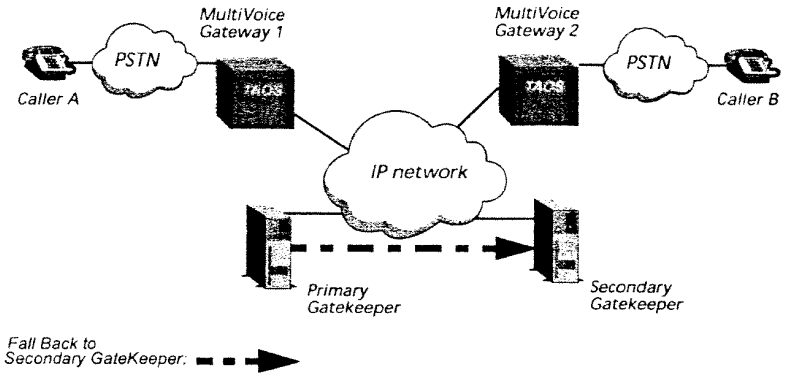
3 When registration is established with the secondary gatekeeper, Gateway 1 forwards the phone number and PIN authentication to the secondary gatekeeper.

4 The secondary gatekeeper authenticates Caller A and, if authentication is successful, forwards the IP address of Gateway 2 to Gateway 1.

5 Gateway 1 establishes a session with Gateway 2.

6 Gateway 2 forwards the call request to Caller B.

Figure 1-5. Example of a MultiVoice network with a secondary gatekeeper



The primary and secondary gatekeepers are separate NT or Solaris-based servers, each with a unique network identity, each running its own copy of the MVAM application, and functioning independently of each other. Each gatekeeper has unique gateway and user databases, and each maintains separate call and activity logs. To ensure coverage, the two gatekeepers must:

- Have duplicate gateway and user information
- Be administered using the same time
- Be synchronized using some third-party clock synchronization mechanism (such as NTP)

The secondary gatekeeper does not report call activity to, nor share call records with the primary gatekeeper. Therefore, if a third-party billing system is used with MultiVoice, all the gatekeepers on the network must communicate with that billing system server.

Increasing gatekeeper reliability

The ITU-T H.323 standard defines a zone as a group of gateways that register with and are administered by a single gatekeeper. Calls may be routed by the gatekeeper directly between any pair of gateways in the same zone.

To maximize gatekeeper reliability, and reliability of a MultiVoice network, multiple MVAM systems, each servicing its own H.323 zone, may be configured as redundant gatekeepers. This is called *sparing*.

In Figure 1-6, MVAM systems in a MultiVoice network are paired for use as reciprocal secondary gatekeepers. Each MVAM serves as both a primary gatekeeper for its selected zone and a secondary gatekeeper for adjoining zones. If a MultiVoice Gateway fails to register with the MVAM in that zone, that gateway attempts to register with its paired MVAM. In this configuration, each gatekeeper maintains duplicate gateway and user information for the reciprocating gatekeeper's zone.

Figure 1-6. Reciprocal secondary gatekeepers

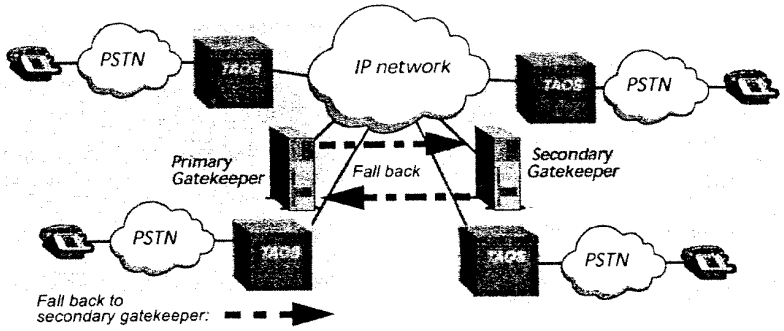
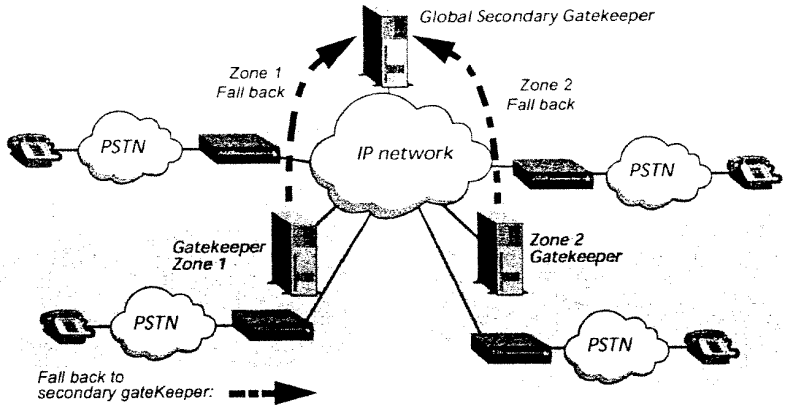


Figure 1-7 illustrates how a MultiVoice network may be configured to use a single MVAM as the secondary gatekeeper for the entire network. If any MultiVoice Gateway fails to register with its primary gatekeeper, that gateway attempts to register with the MVAM performing the global gatekeeper function. The MVAM that performs the global gatekeeper function maintains duplicate gateway and user information for all other gatekeeper zones in the MultiVoice network.

Figure 1-7. Global secondary gatekeeper



Keep-alive registration

Once registered with a gatekeeper, a MultiVoice Gateway must periodically reregister. This is called *keep-alive registration*. Keep-alive registration to informs the gatekeeper that a gateway is available to accept calls. By default, a MultiVoice Gateway attempts keep-alive registration with its primary gatekeeper every 120 seconds. At registration time, the gateway makes up to five registration attempts, at 5-second intervals, until successfully contacting the gatekeeper.

When keep-alive registration fails, the MultiVoice Gateway does one of the following, if:

- A valid IP address (non-null) is configured for the Gatekeeper-Ip-Sec parameter, the gateway attempts to register with its secondary gatekeeper. Once registration is accomplished, the gateway implements the same keep-alive registration policy with the secondary gatekeeper as it did with its primary gatekeeper.
- No valid IP address is configured for the Gatekeeper-Ip-Sec parameter, the gateway goes into a *slow poll mode* with the primary gatekeeper. In this mode the gateway attempts to register with its primary gatekeeper at 30-second intervals, until successfully contacting the gatekeeper.

Note While attempting to register with the primary gatekeeper, the MultiVoice Gateway is effectively *unregistered* with any gatekeeper. During this period, new calls are blocked. However, existing calls continue to operate normally.

Reregistration with a primary gatekeeper

Once the MultiVoice Gateway registers with the secondary gatekeeper, the gateway continues to attempt to reregister with its primary gatekeeper periodically. By default, the gateway makes one attempt to reregister with its primary gatekeeper after every five successful keep-alive registrations with the secondary gatekeeper. After the fifth successful registration with the secondary gatekeeper, the gateway makes up to five registration attempts, at 5-second intervals, to contact its primary gatekeeper. If the MultiVoice Gateway cannot register with its primary gatekeeper after five attempts, the gateway continues to perform keep-alive registration with its secondary gatekeeper.

Gatekeeper registration policy

Gatekeeper registration policy is set on both the MVAM and MultiVoice Gateway. The MultiVoice Access Manager uses the RegistrationDuration parameter to set the interval at which a MultiVoice Gateway must perform keep-alive registration. This parameter defaults to 150 seconds, adding a 30-second buffer to the reregistration interval.

The MultiVoice Gateway uses the following parameters in the `voip { 0 0 }` profile to control gatekeeper registration:

Parameter	Setting
`gatekeeper-ip-sec`	The IP address of the gateway's secondary gatekeeper.
`gatekeeper-keepalive`	The time interval at which a gateway performs keep-alive registration with a gatekeeper.
`registration-retries`	The number of registration attempts a gateway performs during keep-alive registration.
`registration-retry-timer`	The time interval between each registration attempt a gateway performs during keep-alive registration.
`primary-retries`	The number of registrations with the secondary gatekeeper after which a gateway attempts to reregister with its primary gatekeeper. This value represents a cycle of successful keep-alive registrations with the secondary gatekeeper.

For more information about setting gatekeeper registration policy see "H.323 gatekeeper communication" on page 3-24.

How calls are assigned to a MultiVoice gateway

When a call request is received from a gateway, the MVAM first identifies all the gateways which could be used to complete the call. The MVAM may connect calls by selecting a gateway based on the following:

- The available port capacity of each gateway
- The current call volume of each gateway

The selection method is controlled by parameters contained in the MVAM initialization file. See the *MultiVoice Access Manager User's Guide* for a detailed explanation of these parameters.

Call assignment based on port capacity

The MVAM assigns calls based on the available gateway port capacity when configured to do so. As call admission requests (ARQs) are received, the MVAM proceeds as follows:

1 Identifies all the gateways that could possibly connect the call.

2 Checks the ratio of ports in use to ports available for each covering gateway.

3 Selects a gateway with the most available resources for connecting the call (such as, the smallest ratio of ports in use to ports available).

Using the ratio of the gateway's ports in use to the gateway's number of available ports provides better load balancing across gateways with overlapping coverage areas and maximizes the use of available network assets.

Using routing based on port capacity, when three MultiVoice Gateways have the same inclusion area (such as, 516-555-11), the gatekeeper assigns the call to the TAOS unit having the most idle ports (ports available), based on the total port capacity of the gateway.

Call assignment based on call volume

The MVAM assigns calls based on current call volume of each gateway when configured to do so. As call admission requests (ARQs) are received, the MVAM proceeds as follows:

1 Checks the current call volume of each covering gateway.

2 Determines which gateway is connecting the fewest calls.

3 Assigns the call to the gateway currently connecting the fewest calls.

Calls routed based on call volume do not take into account the port capacity of the individual gateway (a port being the combination of a digital signal level 0 (DS0) and digital signal processor (DSP)) how many ports are currently idle and available for connecting calls on a given gateway.

When using the call volume routing, if three MultiVoice Gateways have the same inclusion area (such as, 516-555-11), the gatekeeper assigns the call to the TAOS unit

with the fewest active calls (ports in use), disregarding the total port capacity of that gateway.

Note If the call is rejected by the selected gateway, the call is dropped.

MultiVoice networks supporting multizone call routing

MultiVoice supports routing calls between gateways that are registered with different MVAMs (Gatekeepers). Calls originating at one gateway, registered to and administered by one gatekeeper, are connected using a different gateway that is registered to and administered by another gatekeeper.

The ITU-T H.323 standard defines a zone as a group of gateways that are registered with and administered by a single gatekeeper. Calls may be routed by the gatekeeper directly between any pair of gateways in the same zone.

Routing across H.323 zones

When calls are routed between zones, the gatekeeper in the zone where the call originates contacts a gatekeeper in another zone to locate a gateway to connect the call. When routing between zones, two MVAMs reside on separate servers, each with their own unique set of registered gateways. The two access managers set up the call between two gateways residing in different zones.

Implementing call routing

MVAMs use the optional called endpoint signaling method of call routing, which allows an MVAM to route a call through another gatekeeper.

Each MVAM in a MultiVoice network system maintains a database of peer gatekeepers. Each entry in this database contains a gatekeeper's identifier (a unique name) and its IP address. Each MVAM in the system also has a database of peer gatekeeper inclusion areas.

These inclusion areas define the telephone numbers that a gatekeeper is responsible for covering. Overlapping coverage areas are also supported for gatekeepers.

Figure 1-8 shows an example of a MultiVoice call routed between two gateways in different zones. The gatekeeper MVAM_east requests a call routing for a call originating in New York City to a telephone number in Los Angeles from the gatekeeper MVAM_west, which cannot be connected through an East Coast Zone gateway.

When a MVAM is asked by a gateway to route a call, it first determines if the call can be routed to a gateway within its own zone. If the call cannot be routed within its zone:

1 The East Coast gatekeeper, MVAM_east, receives a request to send a call from the East Coast gatekeeper GW_NY1 to a destination telephone number in Los Angeles, CA.

2 MVAM_east checks its gateway database. It determines that this call cannot be completed through a gateway in the East Coast zone.

3 MVAM_east checks its known gatekeeper database to determine if the coverage area is supported in another zone and locates a coverage area supported by the West Coast gatekeeper, MVAM_west.

4 MVAM_east sends a Location Request message (LRQ) to MVAM_west.

5 MVAM_west checks its gateway database. It determines that its gateway, CA_GW1, can connect the call.

6 MVAM_west sends a Location Confirmed (LCF) message containing the IP address of gateway CA_GW1.

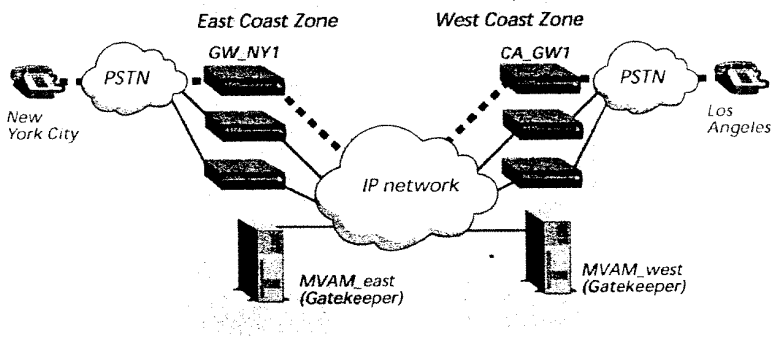
While waiting for a response, MVAM_east sends a Request-In-Progress message to GW_NY1.

7 When MVAM_east receives the Location Confirmed (LCF) message from MVAM_west, an Admission Confirmed (ACF) message containing the conferenceId is sent to GW_NY1.

8 CA_GW1 completes the call.

If the covering gatekeeper decides it does not have a covering gateway, it returns a Location Reject (LRJ) message.

Figure 1-8. Example of a MultiVoice network supporting multizone call routing



While waiting for the covering gatekeeper to respond with gateway information, the MVAM generates pointers to a potential ACF message and the LRQ message in the Active Call Table, and returns without generating an ACF or an Admission Reject (ARJ) message. The LRQ message has the conferenceIdentifier for the call in its nonStandardData parameter, and the covering gatekeeper returns this in the nonStandardData parameter of the LCF or LRJ message.

IP Device Control implementation

IP Device Control (IPDC) is a Media Gateway Control Protocol (MGCP) that is used to connect voice calls originating from the PSTN using a TAOS unit (an APX or MAX TNT). It analyzes incoming data signals, inband control signals and tones, and sets up and controls the appropriate gateways. It also handles management and reporting.

Connection with the SS7 network is achieved through a signaling gateway (SoftSwitch), which provides a traditional SS7 interface to circuit switches and/or

signal transfer points (STPs) and interworks ISDN User Port (ISUP) messages to IPDC. The signaling gateway (SoftSwitch) acts as a media controller, analyzing incoming signals and determining the appropriate backbone network and services required to route the data; controlling point-to-point connections for establishing calls across packet and circuit (PSTN) networks (that is, initiating and managing call setup and release and executing call routing).

Overview of the signaling gateway

The signaling gateway (SoftSwitch) is the call controller and provides an interface to PSTN for signaling using SS7 and it controls MultiVoice Gateways using IPDC.

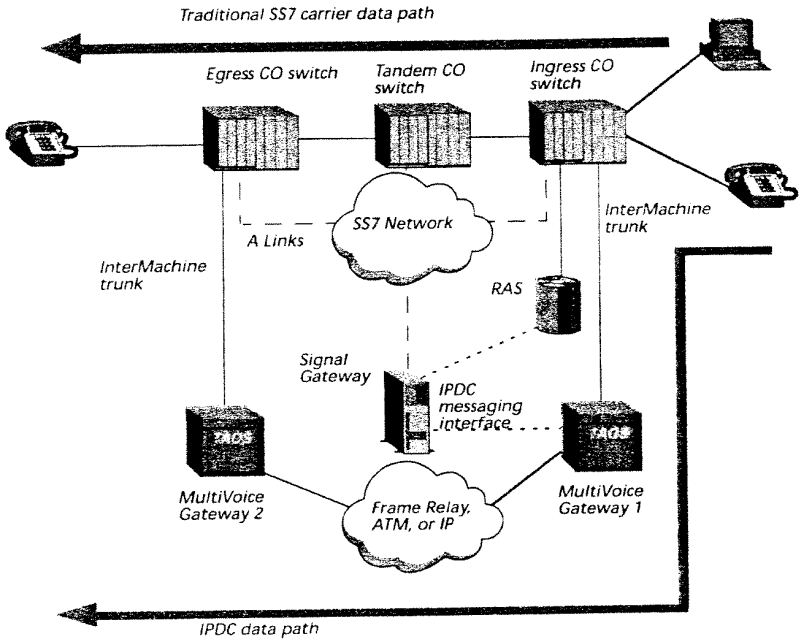
The signaling gateway (SoftSwitch) uses the IPDC protocol to convert SS7 signaling information and call data from the PSTN into IPDC packets, which are sent to the TAOS unit. The signaling gateway (SoftSwitch) also uses IPDC to convert IPDC packets received from a TAOS unit into SS7 messages, before sending the call to the PSTN.

A TAOS unit on the call initiating end uses IPDC to extract Time Division Multiplexing (TDM) and IP routing instructions from the IPDC packets received from the signaling gateway (SoftSwitch) before sending call data across the IP network.

The connecting TAOS unit forwards IPDC packets to the signaling gateway (SoftSwitch), where those packets are converted back into SS7 messages before the call is connected.

Figure 1-9 illustrates the IPDC implementation, which combines a signaling gateway (SoftSwitch) for routing voice, fax and modem calls across a packet network.

Figure 1-9. The Signaling gateway using IPDC implementation



The signaling gateway (SoftSwitch) represents a signal switching point (SSP) node in an SS7 network; which connects, in turn, to a signaling transfer point (STP); which is peered to the core of the signaling network. The signaling gateway (SoftSwitch) uses multiple A-links (v.35, DS-0/A, etc.) to connect to the STP. The remote access server (RAS), on the trunk side, has an intermachine trunk (IMT) (T1, E1, etc.) provisioned from a Class 5 switch. On the line side, the RAS will typically have an ethernet connection to the SG and/or connect through a media controller that will either be integrated with the SG or physically stand alone. The specific configuration depends on the network configuration (that is, ICD, VoIP, Tandem replacement, etc.) and product used for the signaling gateway (SoftSwitch) and media controller.

IPDC call processing messages

IPDC messages exchanged between the TAOS unit and the signaling gateway (SoftSwitch) during VoIP call processing are described in Table 1-1.

Table 1-1. IPDC VoIP call processing messages

Message	Sent by	Purpose
RCCP (Request Confirm Call Parameters)	Signaling gateway (SoftSwitch)	This is a call request message. It contains the call setup information the TAOS unit needs for routing the call to its destination. This includes all IP addressing, RTP port setup, codec and packet loading information.
ACCP (Accept Confirm Call Parameters)	TAOS unit	This is a call confirmation message. It verifies the call setup information the TAOS unit used for routing the call to its destination.
RMCP (Request Modify Call Parameters)	Signaling gateway (SoftSwitch)	This is a request to modify the VoIP call parameters for the current call. It changes call parameters, such as, the active audio codec and switchover to fax, while a VoIP call is in progress.
AMCP (Accept Modify Call Parameters)	TAOS unit	This message confirms modifications to the VoIP call parameters for the current call. It verifies that the requested changes are implemented.
STN (Send Tones Message)	Signaling gateway (SoftSwitch)	This is a call progress message. It directs that certain call-progress tones or voice announcements are played for callers during a VoIP call.
ASTN (acknowledge result of Send Tones Message)	TAOS unit	This message confirms playout of requested call-progress tones or voice announcements during a VoIP call.

Configuration of IPDC messages is performed on the media controller for the signaling gateway (SoftSwitch). One signaling gateway (SoftSwitch) and media controller can manage calls routed through multiple TAOS unit systems.

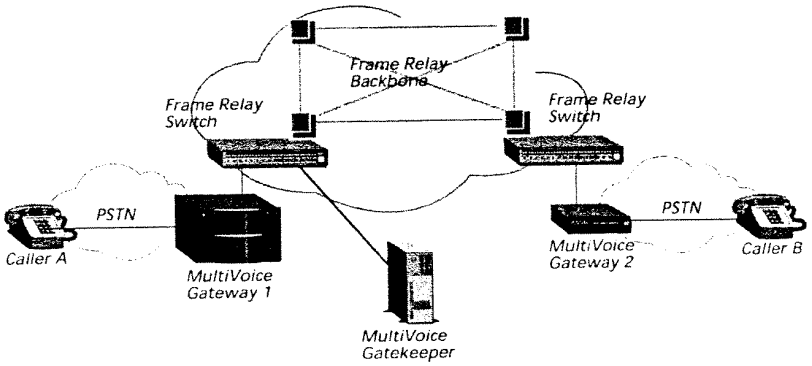
MultiVoice integration with frame relay networks

MultiVoice supports transmission of voice packets across Frame Relay networks as a means of providing improved Quality of Service (QoS). MultiVoice packets can be routed onto a Frame Relay network by connecting through either a router or switch, such as Lucent Technologies Pipeline 85 or Xedia Access Point 45, to the Frame Relay network.

Note While the TAOS unit may be configured as a Frame Relay gateway, MultiVoice is not supported as a Voice over Frame Relay application. It is not recommended that MultiVoice Gateways be used as Frame Relay gateways.

Figure 1-10 shows how MultiVoice Gateways integrate with Frame Relay networks. The MVAM must also be connected to the same Frame Relay backbone network that connects the MultiVoice Gateways.

Figure 1-10. Sample MultiVoice network



MultiVoice applications

MultiVoice supports a variety of applications, including:

- 1+ dialing for residential long distance
- Local toll-free service
- Postpaid and prepaid calling-card service
- PC-to-phone over a virtual private network or an ISP's point of presence (PoP)
- Phone-to-PC (also known as "Internet Call Waiting")
- Single-Stage, 1+ dialing services with interconnection using PSTN or VoIP

1+ dialing for residential long distance

This service is offered for both single-stage and dual-stage dialing of VoIP calls.

With single-stage dialing, the Dialed Number Identification Service (DNIS) string is extracted for the destination telephone number from a single dialed entry. The destination number is passed to the distant gateway during call setup.

With dual-stage dialing, callers are required to dial the MultiVoice Gateway first, then wait for a subsequent dial tone before dialing the called telephone number. The MultiVoice Gateway will prompt the caller for various forms of information, depending on the carrier's service.

MultiVoice solution features

The 1+ dialing for residential long distance application provides the following features:

- PSTN Interconnection — T1 with Feature Group D must be supported.
- Deployable Worldwide — This service is supported in many countries around the world. Check with your Lucent account representative for the comprehensive list of supported countries.
- Compressed Voice and Fax — Multiple encoding schemes are supported. However, most carriers use G.729A codec and real-time fax.
- Transparent Modem — Backhaul of modem sessions over the VoIP network using G.711 must be supported when a modem tone is detected.
- Reliable DTMF with Compressed VoIP — DTMF is recognized on ingress and passed out-of-band in the H.245 user input fields. On egress, the DTMF is generated via the out-of-band DTMF feature.
- Transport of Cause Codes from End-to-End — Carriers use this information to understand the reason why a particular call drops. This information is extremely useful for troubleshooting the application.
- Transport of ANI Info Bits from End-to-End — Requires Feature Group D trunks.
- Single-stage dialing — Requires that the VoIP carrier support Feature Group D or E1 R2 trunks that interface into the ingress side of the PSTN. Subscribers can either dial the carriers' PIC code (for example, 1010-321) or be pre-subscribed in the Central Office (CO) switch by the Local Exchange Carrier (LEC to the VoIP Long-Distance carrier.

Authentication and voice announcements

PIN and ANI authentication can be set up on the MVAM. When dual-stage dialing has been configured on a MultiVoice Gateway, the caller can be prompted to enter a PIN. The following call processing types are supported:

1 Configure ANI authentication. If ANI fails, then prompt for PIN.

2 Configure ANI authentication and only prompt for DNIS.

3 Configure ANI authentication and prompt for PIN and DNIS.

4 Do not configure ANI authentication, but prompt for DNIS.

5 Do not configure ANI authentication, but prompt for PIN and DNIS.

Voice announcements stored on the MultiVoice Gateway provide prompts for the caller. Service providers can customize the creation and installation of these announcements. For details on voice announcements, refer to Chapter 4, "Voice Announcement Administration".

Local toll-free service

For example, local toll-free service (800 or 888) can be much more cost-effective than traditional toll-free service. Typically, leasing charges are less, and MultiVoice technology can eliminate long-distance phone charges.

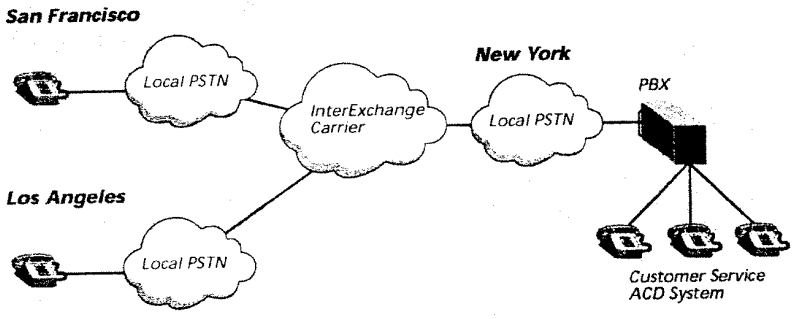
Traditional toll-freeservice

Suppose a company maintains a customer service department, offering their customers a traditional 800 or 888/877 phone number that they dial to receive assistance. Figure 1-11 shows an example of an environment without MultiVoice.

To reach a customer service representative, callers in San Francisco and Los Angeles dial a toll-free phone number that has been leased to a company's customer service department by its InterExchange Carrier (IXC).

The IXC routes the calls to the company's Automatic Call Distributor (ACD) system through a PBX. Because the dialed number is toll-free for the caller, the IXC bills the company for any long-distance charges, in addition to the leasing charges for the toll-free service.

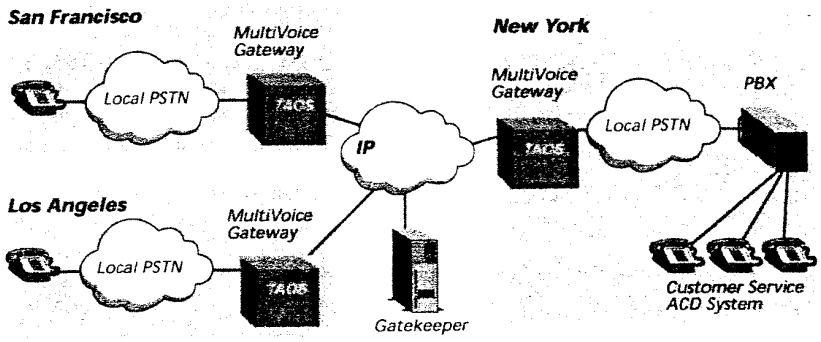
Figure 1-11. Traditional toll-free environment



Using MultiVoice with local toll-free service

Instead of leasing traditional 800 service, supposed the company in Figure 1-12 leases local toll-free service in San Francisco and Los Angeles. Each local PSTN routes local toll-free calls to a local TAOS unit, which forwards them to the customer service site in New York. Figure 1-12 illustrates how a company can use MultiVoice devices and local toll-free service. Typically, leasing charges are less, and MultiVoice technology can eliminate long-distance phone charges.

Figure 1-12. Using MultiVoice with local toll-free service



Postpaid and prepaid calling-card service

Both prepaid and postpaid calling-card services are supported by MultiVoice. With a postpaid calling-card, callers are required to make an access call to the MultiVoice Gateway. Depending on the access number called, the MultiVoice Gateway prompts the caller for various information. The most common call processing types are as follows:

1 Do not configure ANI authentication, but prompt for PIN and DNIS.

2 Configure ANI authentication and prompt for PIN and DNIS.

3 Configure ANI authentication and only prompt for DNIS.

A postpaid calling-card service can be split into multiple services that include a branding requirement. With branding, carriers can have up to two different sets of voice announcements to prompt a caller for the PIN and the DNIS. For example, one set of voice announcements could be recorded and played in the English language and another set could be recorded and played in Spanish.

Prepaid calling-card services provide the same call processing types as the postpaid calling-card service, but provides these additional features as well:

- Provide ANI info bits — This determines call origination (pay phone, prison, or other location and so forth).
- Call Cutoff — When the prepaid call time runs out.
- Play Account Balance.
- Play-Talk-Time-Remaining.
- Play Multiple Low-Balance Warnings.
- Sequential Dialing ("Next Call Please).

The only known limitations of TAOS 9.0 and MVAM 3.1 is the ability to support two languages for Play Account Balance and Play-Talk-Time-Remaining features.

PC-to-phone calls

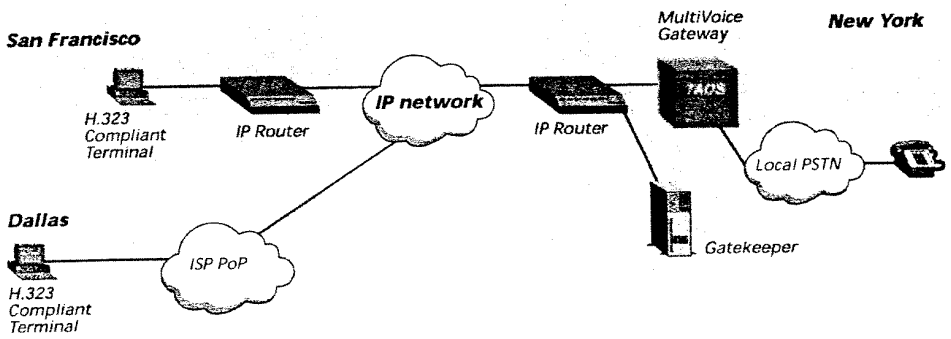
Calls initiated from PCs connected to a network are processed as if the PC was one of the MultiVoice Gateways. This requires that the PC be a fully *H.323-compliant terminal*. It must be able to register and communicate with the gatekeeper as if it were a gateway. It must also be able to communicate with the MultiVoice Gateway at the other end of the call.

Figure 1-13 shows how to PC-to-phone calls could be connected using either a *virtual private network* (VPN) or an ISP's PoP.

The callers in San Francisco use their PCs to place calls to phone numbers in New York from inside the VPN, utilizing the backbone IP network as the link to the destination MultiVoice Gateway.

The callers in Dallas use their PCs to place calls to phone numbers in New York through a local PoP provided by an ISP, utilizing the Internet connection as the link to the destination gateway.

Figure 1-13. Virtual private network using PC telephony



H.323-compliant terminals

H.323-compliant terminals are described in detail in the ITU-T Recommendation H.323. To work with MultiVoice, a PC must use a telephony application which supports:

- Registration, Admission and Status (RAS) messaging with a gatekeeper
- The G.711 audio coder/decoder (required)
- The G.729(a) and G.723.1 audio coder/decoders (optional)

Caution Not all third-party telephony software has full RAS messaging capability, or works with a gatekeeper. Microsoft's NetMeeting, version 3.0, was successfully tested and proven compatible with MultiVoice networks. Calls made from PCs using other applications may fail.

Gateway-to-client keep-alive registration

MultiVoice supports the use of a keep-alive protocol for gateway-to-clients (PCs) and/or gateway-to-gateway connections. This allows the gateway to detect terminated call connections when a remote endpoint becomes unreachable. The

MultiVoice administrator may disable this feature or control the keep-alive time interval through the gateway interface. If the keep-alive timer expires during an active call, the call will be dropped by the gateway and reported to the MVAM with the disconnect reason "forcedDrop."

Phone-to-PC (also known as Internet call waiting)

The Phone-to-PC service allows customers to offer voice call termination from a phone to an Internet user. This is oftentimes referred to as "Internet Call Waiting." To provide this service, the following components are required:

- MultiVoice PC Client (MVC)
- MVAM
- MultiVoice Gateways (APX, MAX TNT)

The MVAM Application Programming Interface (API) also includes an interface to a Lucent RADIUS authentication server. The MVC is used in a standalone format (also known as the cell phone version).

The following explains how the Phone-to-PC service works:

1 Internet users install the MVC on their PC. The MVC installation application can be downloaded from a web page or set to the user on a CD-ROM.

2 Internet users buy/request forward-on-busy from their Local Exchange Carriers (LEC)s. The LECs configure the service to forward calls to the ICW service provider's VoIP network when an Internet user's phone is busy.

3 An Internet user starts a dial-up modem session and is authenticated by RADIUS. The telephone line is now busy.

4 The MVC registers with the customer's MVAM. This alerts MVAM that the user is online and able to accept calls on their PC.

5 Simultaneously, the MVAM API asks the RADIUS server for approval to add the users to the MVAM routing database. Upon approval from RADIUS, the users' routing information is added to MVAM.

6 When a caller dials the Internet user's phone number, the line is busy because the Internet user is online. The call is then forwarded from the LEC to a MultiVoice Gateway in the ICW service provider's network.

7 The MultiVoice Gateway captures the originally dialed number (the number of the Internet user) and routes the call the MVC of the Internet user based on a routing table in MVAM.

8 The Internet user decides to accept or reject the call by clicking a button on the "ringing" MVC user interface.

9 If accepted, the VoIP call path is set up from the MultiVoice Gateway to the MVC using H.323.

10 The user can surf the WWW and talk at the same time.

With the Phone-to-PC service, a RADIUS server provides all user authentication (security) and user provisioning. Although Call Detail Records are available from MVAM (for billing), we recommend that service providers offer this service as a differentiator for their dial-up service customers—as a free or flat-fee offering.

Single-stage, 1+ dialing with interconnection using PSTN or VoIP

MultiVoice supports interconnection to other networks. These interfaces can be via PCM using standard PSTN trunking or via VoIP. The various forms of network interconnection include:

- MultiVoice Gatekeeper-to-Gatekeeper communications
- MultiVoice Gatekeeper-to-Gatekeeper communications with AT&T Harvester
- MultiVoice Gatekeeper-to-Clearinghouse using the Open Settlement Protocol (OSP)

MultiVoice solution features

Similar to the 1+ dialing for residential long distance application, the features for this service include the following:

- PSTN Interconnection — T1, T3, E1, CAS, PRI, R2, Feature Group D.
- Deployable Worldwide — This service is supported in many countries around the world. Check with your Lucent account representative for the comprehensive list of supported countries.
- Compressed Voice and Fax — Multiple encoding schemes are supported. However, most carriers use G.729A codec and real-time fax.
- Transparent Modem — Backhaul of modem sessions over the VoIP network using G.711 must be supported when a modem tone is detected.
- Reliable DTMF with Compressed VoIP — DTMF is recognized on ingress and passed out-of-band in the H.245 user input fields. On egress, the DTMF is generated via the out-of-band DTMF feature.
- Transport of Cause Codes from End-to-End — Carriers use this information to understand the reason why a particular call drops. This information is extremely useful for troubleshooting the application.
- Transport of ANI Info Bits from End-to-End — Requires Feature Group D trunks.

MultiVoice Gateway Configuration

2

System configuration

To use a TAOS unit as a MultiVoice Gateway, it must be

- Licensed to provide the appropriate feature support for VoIP call processing
- Configured to process audio signals for VoIP calls
- Configured to allow the TAOS unit to be recognized and communicate as a MultiVoice Gateway

Caution MultiVoice does not work on a multishelf MAX TNT. Before installing MultiVoice on a multishelf MAX TNT, it must be reconfigured as a single-shelf unit.

Base profile parameters

TAOS unit support for VoIP is determined by settings on the shelf controller. The settings are displayed in the read-only base profile. The parameters that specify VoIP functionality follow.

Parameter	Setting
`voip-enabled`	Enables VoIP call processing. When this parameter is set to yes, the TAOS unit has been licensed to process VoIP calls.
`voip-max-capacity-allowed`	Sets the maximum VoIP call processing limit for an APX. When this parameter is set to yes, the VoIP software license imposes a limit on the maximum number of simultaneous VoIP calls an APX can process, regardless of how many DS3, T3, MultiDSP, or Ethernet slot cards are installed. This parameter is always set to no on a MAX TNT.
`xcom-ss7`	Enables/disables IPDC processing on an APX or a MAX TNT. When this parameter is set to enabled, the TAOS unit has been licensed to perform IPDC packet processing, in support of SS7 networks. The parameter value must be set to enabled to perform IPDC VoIP.

The `voip-max-capacity-allowed` parameter imposes a limit (that is, 2688 VoIP calls) on APX resources allocated for processing VoIP calls. This parameter works in conjunction with the default setting of the `maxcalls` parameter in the `voip` profile (see "Controlling VoIP call volume" on page 3-20 for details).

In multiple application environments (where both data and VoIP calls are processed by the same APX), this parameter allows you to scale VoIP support to match demand for VoIP services.

Note If an APX is licensed to process up to 2688 VoIP calls, VoIP call request 2689 is rejected.

To display all parameters in the read-only base profile, do the following:

```
admin> get base
[in BASE]
shelf-number = 1
software-version 9
.....
voip-enabled = yes
voip-max-capacity-allowed = yes
.....
```

Note These are read-only parameters that cannot be changed without relicensing the MultiVoice Gateway.

Configured memory requirements

The MAX TNT requires installation of a 32Mb JEDEC DRAM slot card and an 8Mb flash card to boot up and function properly.

The APX requires installation of a 32Mb flash card to boot up and function properly.

Using slot cards in a MultiVoice Gateway

The next few sections discuss slot cards that can be (or must be) installed in a MultiVoice Gateway. After you have installed a slot card, use the show command to verify the card is operational. For example:

```
admin> show
Shelf 1 ( standalone ):
                          Reqd    Oper    Slot Type
   { shelf-1 slot-1 0 } UP      UP      ether3nd-card
   { shelf-1 slot-2 0 } UP      UP      madd3-card
   { shelf-1 slot-5 0 } UP      UP      t3-card
```

MultiDSP slot cards

To use an APX or a MAX TNT as a MultiVoice Gateway, you need to install a MultiDSP slot card. A MultiDSP card is a single-slot card that supports VoIP services. A digital signal processor (DSP) is specially optimized for signal processing.

Each DSP has two channels, but when running a VoIP session, only one channel is used per call. The second channel cannot be used. A VoIP session removes the sister channel from the available list.

Two MultiDSP slot cards are available for use with MultiVoice:

- 48-port MultiDSP slot card (TNTV-SL-ADI-C)
- 96-port MultiDSP slot card (APX8-SL-96DSP)

Both slot cards can handle up to two services per slot card. The 48-port MultiDSP slot card supports 48 ports of any service. When running two services per slot card, the services can be used only in one of the following combinations:

- Data (modem/ISDN) with V.110
- Data (modem/ISDN) with Personal Handyphone System (PHS)
- Data (modem/ISDN) with VoIP

The 96-port MultiDSP slot card currently supports 96 ports of data (modem/ISDN) and/or V.110 service. When running two services per slot card, one service must be data and the other must be V.110.

Mixing MultiDSP slot cards

For H.323, if both 48-port (TNTV-SL-ADI-C) and 96-port (APX8-SL-96DSP) MultiDSP slots cards are enabled in the same chassis, only simple codecs (that is, G.711 and G.729) are permitted. H.323 VoIP calls use codecs that are supported by ALL MultiDSP cards enabled in the chassis.

If the 288-port slot card is configured to use 480 ports, then only the G.711 codec is supported for all slot cards. Enabling a 480-port card limits the H.323 codec selection

to G.711. Enabling a 96-port card limits the codecs to G.711 and G.729. See "Configuring 480 ports for G.711-encoded VoIP-only calls" on page 2-65 for details.

If using IPDC, both simple (that is, G.711 and G.729) and complex (that is, G.723, G.723-6.4kps, G.728, and FRGSM) codecs are supported if at least one card in the chassis supports the desired codec. If a gateway has both a 480-port card and a 288-port card, then IPDC VoIP calls can be made using G.711, G.729, and G.723 codecs. In order to support G.728 and FRGSM, a 48-port card needs to be enabled.

Slot card restrictions

The following configuration restrictions apply to both APX and MAX TNT units used as MultiVoice Gateways:

- The dual-port Series56™ Digital Modem slot card (TNT-SL-48MOD-S56) cannot be used in the same TAOS unit with MultiDSP slot cards.
- Multiple 48-port MultiDSP cards can be used in the same TAOS unit.
- The Series56™ II (TNT-SL-48MOD-SGL and TNT-SL-48MOD-S-C) and the Series56™ III (TNT-SL-48MODV3-S-C) Digital Modem slot cards can be used in the same TAOS unit with MultiDSP slot cards.

For installation information, see the *APX 8000 Hardware Installation Guide*, the *MAX TNT Hardware Installation Guide*, and the *APX 8000/MAX TNT Physical Interface Configuration Guide*. Profile configuration procedures are described in the *APX 8000/MAX TNT Physical Interface Configuration Guide* and the *TAOS Command-Line Interface Guide*.

When a TAOS unit detects the presence of a slot card in one of its slots, the TAOS unit creates default profiles that are specific to that type of slot card. Each profile is indexed by its physical address (shelf number, slot number, and item number) within the TAOS unit. You might need to reconfigure default profiles when a new slot card is installed.

Cohabitation on a single DSP

Cohabitation refers to the ability to run multiple applications on a single DSP. Cohabitation can be configured in the following combinations:

- One VoIP session using either the G.729A or G.711 audio codec, and one modem session
- Two VoIP sessions using either the G.729A or G.711 audio codec
- Two modem sessions

StrongARM processor

Cohabitation enables a MultiVoice Gateway to support multiple application processing on the same platform for a combination voice and data calls. During the call setup process, the StrongARM processor allocates DSPs to either voice or data calls depending upon the following:

- Call type
- Requested audio codec
- Available DSP channels

Cohabitation is restricted to performing VoIP calls plus one other data call type (such as a modem call).

DSP allocation

As call requests are processed by the MultiVoice Gateway, the StrongARM processor on the MultiDSP slot card checks each incoming call to determine an application type and subtype. Application type and subtype determines how DSPs are allocated for that call. Modem and VoIP calls, regardless of the audio codec requested, have the same application type. The application subtype is different for the complex audio codecs.

Modem, G.729, and G.711 calls all belong to the modem application type and have no application subtype. For cohabitation processing, when the modem application type is detected, only one DSP channel is allocated for the call. The twin channel on the DSP is assigned the value of no application subtype and is considered available for processing other calls.

When a 48-port MultiDSP slot card is being used, calls using G.723, G.728, and Full-Rate GSM codecs have the application subtype VOIP. When that application subtype is detected, a whole DSP is allocated for the call.

Audio codec selection

Audio codec selection is determined during H.245 terminal capabilities between the two TAOS units that connect a call. When the call request is received by the MultiDSP slot card, the call is brought up initially as a modem application type. If the call request asks for one of the complex audio codecs, the complex codec is loaded on a DSP where both channels are available.

Ethernet-3 slot card

APX and MAX TNT units do not support routing of VoIP calls through the shelf-controller Ethernet port. Instead, the Ethernet-3 slot card (TNT-SL-E100-V-C), a high-performance Ethernet module with one 100Mbps interface, is used for routing VoIP call data between TAOS units.

For installation information see the *Hardware Installation Guide* for your TAOS unit. For descriptions of profile configuration procedures see the *APX 8000/MAX TNT Physical Interface Configuration Guide* and the *TAOS Command-Line Interface Guide.*

Enabling full-duplex mode

When using the Ethernet-3 slot card to support VoIP call processing, the slot card must operate in full-duplex mode. The card operates in full-duplex mode by default, as specified in the setting of the following parameter in the ethernet profile:

```
[in ETHERNET/{ any-shelf any-slot 0 }]
duplex-mode = full-duplex
```

Configuring connecting ports on the packet switch or router

The 100Mbps interface on the Ethernet-3 slot card is not auto configurable Do not connect it to a hub or router port that has auto negotiation enabled. Connecting the Ethernet-3 card interface to an auto negotiated port can have negative effects on VoIP